

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
amarok -- amarok	Multiple integer overflows in the Audible::Tag::readTag function in metadata/audible/audibletag.cpp in Amarok 1.4.10 through 2.0.1 allow remote attackers to execute arbitrary code via an Audible Audio (.aa) file with a large (1) nlen or (2) vlen Tag value, each of which triggers a heap-based buffer overflow.	2009-01-16	9.3	CVE-2009-0135 CONFIRM CONFIRM SECTRACK BUGTRAQ FRSIRT CONFIRM CONFIRM MISC SECUNIA MLIST CONFIRM CONFIRM
amarok -- amarok	Multiple array index errors in the Audible::Tag::readTag function in metadata/audible/audibletag.cpp in Amarok 1.4.10 through 2.0.1 allow remote attackers to cause a denial of service (application crash) or execute arbitrary code via an Audible Audio (.aa) file with a crafted (1) nlen or (2) vlen Tag value, each of which can lead	2009-01-16	9.3	CVE-2009-0136 CONFIRM CONFIRM SECTRACK BUGTRAQ FRSIRT CONFIRM CONFIRM CONFIRM

	to an invalid pointer dereference, or the writing of a 0x00 byte to an arbitrary memory location, after an allocation failure.		MISC SECUNIA MLIST CONFIRM CONFIRM	
apple -- quicktime	Heap-based buffer overflow in Apple QuickTime before 7.6 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via a crafted RTSP URL.	2009-01-21	9.3	CVE-2009-0001 APPLE
apple -- quicktime	Heap-based buffer overflow in Apple QuickTime before 7.6 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via a QTVR movie file with crafted THKD atoms.	2009-01-21	9.3	CVE-2009-0002 APPLE
apple -- quicktime	Heap-based buffer overflow in Apple QuickTime before 7.6 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via a crafted AVI movie file.	2009-01-21	9.3	CVE-2009-0003 APPLE
apple -- quicktime	Buffer overflow in Apple QuickTime before 7.6 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via a crafted MP3 audio file.	2009-01-21	9.3	CVE-2009-0004 APPLE
apple -- quicktime	Unspecified vulnerability in Apple QuickTime before 7.6 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via a crafted H.263 encoded movie file that triggers memory corruption.	2009-01-21	9.3	CVE-2009-0005 APPLE
apple -- quicktime	Integer signedness error in Apple QuickTime before 7.6 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via a crafted Cinepak encoded movie file that triggers a heap-based buffer overflow.	2009-01-21	9.3	CVE-2009-0006 APPLE
apple -- quicktime	Heap-based buffer overflow in Apple QuickTime before 7.6 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via a QuickTime movie file containing crafted JPEG atoms.	2009-01-21	9.3	CVE-2009-0007 APPLE

apple -- quicktime_mpeg_2_playback_component	Unspecified vulnerability in Apple QuickTime MPEG-2 Playback Component before 7.60.92.0 on Windows allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a crafted MPEG-2 movie.	2009-01-22	7.6	CVE-2009-0008 BID CONFIRM APPLE
asp-dev -- xm_events_diary	SQL injection vulnerability in default.asp in ASP-DEv XM Events Diary allows remote attackers to execute arbitrary SQL commands the cat parameter.	2009-01-21	7.5	CVE-2008-5923 BID SECUNIA MISC
asp-dev -- xm_events_diary	SQL injection vulnerability in diary_viewC.asp in ASP-DEv XM Events Diary allows remote attackers to execute arbitrary SQL commands via the cat parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-01-21	7.5	CVE-2008-5924 SECUNIA
asp-dev -- internal_email_system	Multiple SQL injection vulnerabilities in login.asp in ASP-DEv Internal E-Mail System allow remote attackers to execute arbitrary SQL commands via the (1) login parameter (aka user field) or the (2) password parameter (aka pass field). NOTE: some of these details are obtained from third party information.	2009-01-21	7.5	CVE-2008-5926 BID MILWORM SECUNIA
cfagcms -- cfagcms	Multiple PHP remote file inclusion vulnerabilities in themes/default/index.php in Cant Find A Gaming CMS (CFAGCMS) 1 allow remote attackers to execute arbitrary PHP code via a URL in the (1) main and (2) right parameters.	2009-01-21	7.5	CVE-2008-5922 BID MILWORM
china-on-site -- flexphpnews	Multiple SQL injection vulnerabilities in admin/usercheck.php in FlexPHPNews 0.0.6 allow remote attackers to execute arbitrary SQL commands via the (1) checkuser parameter (aka username field) or (2) checkpass parameter (aka password field) to admin/index.php. NOTE: some of these details are obtained from third party information.	2009-01-21	7.5	CVE-2008-5927 BID MILWORM SECUNIA
cisco -- ons cisco -- ons_15600	Cisco ONS 15310-CL, 15310-MA, 15327, 15454, 15454 SDH, and 15600 with software 7.0.2 through 7.0.6, 7.2.2, 8.0.x, 8.5.1, and 8.5.2 allows remote attackers to cause a denial of service	2009-01-16	7.8	CVE-2008-3818 XF BID CISCO

	(control-card reset) via a crafted TCP session.			CISCO SECTRACK
cisco -- unified_ip_phone_7940g cisco -- unified_ip_phone_7960g	Cisco Unified IP Phone (aka SIP phone) 7960G and 7940G with firmware P0S3-08-9-00 and possibly other versions before 8.10 allows remote attackers to cause a denial of service (device reboot) or possibly execute arbitrary code via a Realtime Transport Protocol (RTP) packet with malformed headers.	2009-01-16	7.1	CVE-2008-4444 XF BID BUGTRAQ CONFIRM
cmsisweb -- cms_isweb	SQL injection vulnerability in index.php in CMS ISWEB 3.0 allows remote attackers to execute arbitrary SQL commands via the id_sezione parameter.	2009-01-21	7.5	CVE-2008-5934 BID MILWORM SECUNIA
easyhdr -- easyhdr	Stack-based buffer overflow in easyHDR PRO 1.60.2 allows user-assisted attackers to execute arbitrary code via an invalid Radiance RGBE (aka .hdr) file.	2009-01-22	9.3	CVE-2009-0246 BUGTRAQ MISC SECUNIA CONFIRM
easyhdr -- easyhdr	Stack-based buffer overflow in easyHDR PRO 1.60.2 allows user-assisted attackers to execute arbitrary code via an invalid Flexible Image Transport System (FITS) file. NOTE: some of these details are obtained from third party information.	2009-01-22	9.3	CVE-2009-0254 SECUNIA CONFIRM
enthallweb -- ereservations	Multiple SQL injection vulnerabilities in default.asp in Enthrallweb eReservations allow remote attackers to execute arbitrary SQL commands via the (1) Login parameter (aka username field) or the (2) Password parameter (aka password field). NOTE: some of these details are obtained from third party information.	2009-01-22	7.5	CVE-2009-0252 XF BID MILWORM SECUNIA
flds-script -- flds	SQL injection vulnerability in redir.php in Free Links Directory Script (FLDS) 1.2a allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-01-21	7.5	CVE-2008-5928 BID MILWORM SECUNIA
ganglia -- ganglia	Stack-based buffer overflow in the process_path function in gmetad/server.c in Ganglia 3.1.1 allows remote attackers to cause a denial of service (crash) via a request to the gmetad service with a long pathname.	2009-01-21	7.5	CVE-2009-0241 BID MLIST SECUNIA MISC

ganglia -- ganglia	Ganglia 3.1.1 allows remote attackers to cause a denial of service via a request to the gmetad service with a path does not exist, which causes Ganglia to (1) perform excessive CPU computation and (2) send the entire tree, which consumes network bandwidth.	2009-01-21	7.8	CVE-2009-0242 MLIST
git -- git	The web interface in git (gitweb) 1.5.x before 1.5.5 allows remote attackers to execute arbitrary commands via shell metacharacters related to git_search.	2009-01-20	7.5	CVE-2008-5516 CONFIRM CONFIRM BUGTRAQ MLIST MLIST DEBIAN CONFIRM MISC SUSE CONFIRM
heathcosoft -- mp3_trackmaker	Heap-based buffer overflow in Heathco Software MP3 TrackMaker 1.5 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a long string in an invalid .mp3 file.	2009-01-20	9.3	CVE-2009-0175 XF BID MILWORM
ibm -- hardware_management_console	Unspecified vulnerability in IBM Hardware Management Console (HMC) 7 release 3.2.0 SP1 has unknown impact and attack vectors.	2009-01-20	10.0	CVE-2009-0178 XF CONFIRM BID FRSIRT SECUNIA OSVDB
joey_schulze -- mod_auth_mysql	SQL injection vulnerability in mod_auth_mysql.c in the mod-auth-mysql (aka libapache2-mod-auth-mysql) module for the Apache HTTP Server 2.x allows remote attackers to execute arbitrary SQL commands via multibyte character encodings for unspecified input.	2009-01-22	7.5	CVE-2008-2384 CONFIRM
microsoft -- windows_2000_microsoft	Microsoft Windows does not properly enforce the Autorun and NoDriveTypeAutoRun registry values, which allows physically proximate attackers to execute arbitrary code by (1) inserting CD-ROM media, (2) inserting DVD media, (3) connecting a USB device, and (4) connecting a			

microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Firewire device; (5) allows user-assisted remote attackers to execute arbitrary code by mapping a network drive; and allows user-assisted attackers to execute arbitrary code by clicking on (6) an icon under My Computer\Devices with Removable Storage and (7) an option in an AutoPlay dialog, related to the Autorun.inf file. NOTE: vectors 1 and 3 on Vista are already covered by CVE-2008-0951.	2009-01-21	7.2	CVE-2009-0243 CERT MISC	
microsoft -- windows_mobile	Directory traversal vulnerability in the OBEX FTP Service in the Microsoft Bluetooth stack in Windows Mobile 6 Professional, and probably Windows Mobile 5.0 for Pocket PC and 5.0 for Pocket PC Phone Edition, allows remote authenticated users to list arbitrary directories, and create or read arbitrary files, via a .. (dot dot) in a pathname. NOTE: this can be leveraged for code execution by writing to a Startup folder.	2009-01-21	8.5	CVE-2009-0244 MISC BID BUGTRAQ	
navboard -- navboard	Multiple directory traversal vulnerabilities in NavBoard 16 (2.6.0) allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the module parameter to (1) admin_modules.php and (2) modules.php.	2009-01-22	7.5	CVE-2008-5943 BID SECUNIA MISC	
nfs -- nfs-utils	Certain Fedora build scripts for nfs-utils before 1.1.2-9.fc9 on Fedora 9, and before 1.1.4-6.fc10 on Fedora 10, omit TCP Wrapper support, which might allow remote attackers to bypass intended access restrictions, possibly a related issue to CVE-2008-1376.	2009-01-20	7.5	CVE-2009-0180 FEDORA FEDORA CONFIRM XF BID SECUNIA	
nukevietcms -- nukeviet	Nukeviet 2.0 Beta allows remote attackers to bypass authentication and gain administrative access by setting the admf cookie to 1. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-01-22	7.5	CVE-2008-5945 BID	
	The Word processor in OpenOffice.org 1.1.2 through 1.1.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary			CVE-2009-0259	

openoffice -- openoffice.org	code via a crafted (1) .doc, (2) .wri, or (3) .rtf Word 97 file that triggers memory corruption, as exploited in the wild in December 2008, as demonstrated by 2008-crash.doc.rar, and a similar issue to CVE-2008-4841.	2009-01-22	9.3	U2J2 MLIST MILWORM MISC
php-fusion -- php-fusion	SQL injection vulnerability in readmore.php in PHP-Fusion 4.01 allows remote attackers to execute arbitrary SQL commands via the news_id parameter.	2009-01-22	7.5	CVE-2008-5946 MISC BID
realnetworks -- helix_server realnetworks -- helix_server_mobile	Multiple buffer overflows in RealNetworks Helix Server and Helix Mobile Server 11.x before 11.1.8 and 12.x before 12.0.1 allow remote attackers to (1) cause a denial of service via three crafted RTSP SETUP commands, or execute arbitrary code via (2) an NTLM authentication request with malformed base64-encoded data, (3) an RTSP DESCRIBE command, or (4) a DataConvertBuffer request.	2009-01-20	10.0	CVE-2008-5911 SECTRACK SECTRACK SECTRACK SECTRACK FRSIRT SECUNIA CONFIRM
realvnc -- realvnc	The CMsgReader::readRect function in the VNC Viewer component in RealVNC VNC Free Edition 4.0 through 4.1.2, Enterprise Edition E4.0 through E4.4.2, and Personal Edition P4.0 through P4.4.2 allows remote VNC servers to execute arbitrary code via crafted RFB protocol data, related to "encoding type."	2009-01-16	10.0	CVE-2008-4770 CONFIRM
research_in_motion_limited -- blackberry_enterprise_server research_in_motion_limited -- blackberry_professional_software research_in_motion_limited -- blackberry_unite	Multiple heap-based buffer overflows in the PDF distiller in the Attachment Service in Research in Motion (RIM) BlackBerry Enterprise Server (BES) 4.1.3 through 4.1.6, BlackBerry Professional Software 4.1.4, and BlackBerry Unite! before 1.0.3 bundle 28 allow user-assisted remote attackers to execute arbitrary code via (1) a crafted stream in a .pdf file, related to "symWidths"; or (2) a crafted data stream in a .pdf file, related to "bitmaps."	2009-01-20	9.3	CVE-2009-0176 BID CONFIRM CONFIRM SECUNIA IDEFENSE IDEFENSE
research_in_motion_limited -- blackberry_enterprise_server research_in_motion_limited -- blackberry_professional_software	The PDF distiller in the Attachment Service in Research in Motion (RIM) BlackBerry Enterprise Server (BES) 4.1.3 through 4.1.6, BlackBerry Professional Software 4.1.4, and BlackBerry Unite! before 1.0.3 bundle	2009-01-20	9.3	CVE-2009-0219 CONFIRM CONFIRM

blackberry_professional_software_research_in_motion_limited -- blackberry_unite	28 performs delete operations on uninitialized pointers, which allows user-assisted remote attackers to execute arbitrary code via a crafted data stream in a .pdf file.	20	CONFIRM SECUNIA IDEFENSE
share2 -- easy_grid_control	Insecure method vulnerability in the EasyGrid.SGCtrl.32 ActiveX control in EasyGrid.ocx 1.0.0.1 in AAA EasyGrid ActiveX 3.51 allows remote attackers to create and overwrite arbitrary files via the (1) DoSaveFile or (2) DoSaveHtmlFile method. NOTE: vector 1 could be leveraged for code execution by creating executable files in Startup folders or by accessing files using hcp:// URLs. NOTE: some of these details are obtained from third party information.	2009-01-16	9.3 CVE-2009-0134 XF BID MILWORM SECUNIA
sun -- opensolaris	Unspecified vulnerability in conv_lpd in Sun OpenSolaris has unknown impact and local attack vectors, related to improper handling of temporary files, aka Bug ID 6655641.	2009-01-16	7.2 CVE-2008-5909 MISC
sun -- opensolaris	Unspecified vulnerability in txzonemgr in Sun OpenSolaris has unknown impact and local attack vectors, related to a "Temporary file vulnerability," aka Bug ID 6653462.	2009-01-16	7.2 CVE-2008-5910 MISC
sun -- java_system_access_manager	Sun Java System Access Manager 7.1 allows remote authenticated sub-realm administrators to gain privileges, as demonstrated by creating the amadmin account in the sub-realm, and then logging in as amadmin in the root realm.	2009-01-16	9.0 CVE-2009-0169 BID CONFIRM
symantec -- appstream_client	The LaunchObj ActiveX control before 5.2.2.865 in launcher.dll in Symantec AppStream Client 5.2.x before 5.2.2 SP3 MP1 does not properly validate downloaded files, which allows remote attackers to execute arbitrary code via the installAppMgr method and unspecified other methods.	2009-01-20	9.3 CVE-2008-4388 CERT-VN
the_net_guys -- aspired2blog	SQL injection vulnerability in admin/blog_comments.asp in The Net Guys ASPired2Blog allows remote attackers to execute arbitrary SQL commands via the BlogID parameter.	2009-01-21	7.5 CVE-2008-5930 XF BID MILWORM SECUNIA
	The create_anchors function in utils.inc		CVE-2009

tigris -- websvn	in WebSVN 1.x allows remote attackers to execute arbitrary PHP code via a crafted username that is processed by the preg_replace function with the eval switch.	2009-01-20	7.5	CVE-2000-5920 BID MILWORM MISC
trend_micro -- internet_security_2007 trend_micro -- internet_security_2008 trend_micro -- officescan	Multiple heap-based buffer overflows in the ApiThread function in the firewall service (aka TmPfw.exe) in Trend Micro Network Security Component (NSC) modules, as used in Trend Micro OfficeScan 8.0 SP1 Patch 1 and Internet Security 2007 and 2008 17.0.1224, allow remote attackers to execute arbitrary code via a packet with a small value in an unspecified size field.	2009-01-21	10.0	CVE-2008-3865 BID
typo3 -- typo3	Session fixation vulnerability in the authentication library in TYPO3 4.0.0 through 4.0.9, 4.1.0 through 4.1.7, and 4.2.0 through 4.2.3 allows remote attackers to hijack web sessions via unspecified vectors related to (1) frontend and (2) backend authentication.	2009-01-22	7.5	CVE-2009-0256 XF BID CONFIRM SECUNIA
typo3 -- typo3	Unspecified vulnerability in the Indexed Search Engine (indexed_search) system extension in TYPO3 4.0.0 through 4.0.9, 4.1.0 through 4.1.7, and 4.2.0 through 4.2.3 allows remote attackers to execute arbitrary commands via unknown vectors related to the command-line indexer.	2009-01-22	10.0	CVE-2009-0258 XF BID CONFIRM SECUNIA
umerinc -- songs_portal	SQL injection vulnerability in albums.php in Umer Inc Songs Portal allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-01-21	7.5	CVE-2008-5921 XF BID MILWORM
vuplayer -- vuplayer	Stack-based buffer overflow in VUPlayer 2.49 allows remote attackers to execute arbitrary code via a long .asf URI in the HREF attribute of a REF element in a .asx file.	2009-01-20	9.3	CVE-2009-0174 XF BID MILWORM MILWORM MILWORM MILWORM
vuplayer -- vuplayer	Buffer overflow in VUPlayer allows user-assisted attackers to have an unknown impact via a long file, as demonstrated by a file composed	2009-01-20	9.3	CVE-2009-0181 BUGTRAQ

	entirely of 'A' characters.			
vuplayer -- vuplayer	Buffer overflow in VUPlayer 2.49 and earlier allows user-assisted attackers to execute arbitrary code via a long URL in a File line in a .pls file, as demonstrated by an http URL on a File1 line.	2009-01-20	9.3	CVE-2009-0182 MILWORM
zkesoft -- ayeview	AyeView 2.20 allows user-assisted attackers to cause a denial of service (memory consumption or application crash) via a bitmap (aka .bmp) file with large height and width values.	2009-01-21	7.8	CVE-2008-5937 MILWORM

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
53kf -- web_im_2009	The server for 53KF Web IM 2009 Home, Professional, and Enterprise editions relies on client-side protection mechanisms against cross-site scripting (XSS), which allows remote attackers to conduct XSS attacks by using a modified client to send a crafted IM message, related to the msg variable.	2009-01-22	4.3	CVE-2009-0247 XF BID BUGTRAQ
apache -- jackrabbit	Multiple cross-site scripting (XSS) vulnerabilities in Apache Jackrabbit before 1.5.2 allow remote attackers to inject arbitrary web script or HTML via the q parameter to (1) search.jsp or (2) swr.jsp.	2009-01-21	4.3	CVE-2009-0026 CONFIRM XF BID BUGTRAQ SECUNIA
asp-dev -- xm_events_diary	ASP-DEv XM Events Diary stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for diary.mdb.	2009-01-21	5.0	CVE-2008-5925 MISC
cisco -- ios cisco -- ios	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP server in Cisco IOS 11.0 through 12.4 allow remote attackers to inject arbitrary web script or HTML via (1) the query string to the ping program or (2) unspecified other aspects of the URI.	2009-01-16	4.3	CVE-2008-3821 XF BID BUGTRAQ MISC CISCO SECTRACK JVN
	PXE Encryption in Cisco IronPort Encryption Appliance 6.2.4 before			

cisco -- ironport_encryption_appliance cisco -- ironport_postx	6.2.4.1.1, 6.2.5, 6.2.6, 6.2.7 before 6.2.7.7, 6.3 before 6.3.0.4, and 6.5 before 6.5.0.2; and Cisco IronPort PostX 6.2.1 before 6.2.1.1 and 6.2.2 before 6.2.2.3; allows remote attackers to obtain the decryption key via unspecified vectors, related to a "logic error."	2009-01-16	4.3	CVE-2009-0053 BID CISCO SECTRACK
cisco -- ironport_encryption_appliance cisco -- ironport_postx	PXE Encryption in Cisco IronPort Encryption Appliance 6.2.4 before 6.2.4.1.1, 6.2.5, 6.2.6, 6.2.7 before 6.2.7.7, 6.3 before 6.3.0.4, and 6.5 before 6.5.0.2; and Cisco IronPort PostX 6.2.1 before 6.2.1.1 and 6.2.2 before 6.2.2.3; allows remote attackers to capture credentials by tricking a user into reading a modified or crafted e-mail message.	2009-01-16	4.3	CVE-2009-0054 BID CISCO SECTRACK
cisco -- ironport_encryption_appliance cisco -- ironport_postx	Cross-site request forgery (CSRF) vulnerability in the administration interface in Cisco IronPort Encryption Appliance 6.2.4 before 6.2.4.1.1, 6.2.5, 6.2.6, 6.2.7 before 6.2.7.7, 6.3 before 6.3.0.4, and 6.5 before 6.5.0.2; and Cisco IronPort PostX 6.2.1 before 6.2.1.1 and 6.2.2 before 6.2.2.3; allows remote attackers to modify appliance preferences as arbitrary users via unspecified vectors.	2009-01-16	6.8	CVE-2009-0055 BID CISCO SECTRACK
cisco -- ironport_encryption_appliance cisco -- ironport_postx	Cross-site request forgery (CSRF) vulnerability in the administration interface in Cisco IronPort Encryption Appliance 6.2.4 before 6.2.4.1.1, 6.2.5, 6.2.6, 6.2.7 before 6.2.7.7, 6.3 before 6.3.0.4, and 6.5 before 6.5.0.2; and Cisco IronPort PostX 6.2.1 before 6.2.1.1 and 6.2.2 before 6.2.2.3; allows remote attackers to execute commands and modify appliance preferences as arbitrary users via a logout action.	2009-01-16	6.8	CVE-2009-0056 BID CISCO SECTRACK
cisco -- security_manager	Cisco Security Manager 3.1 and 3.2 before 3.2.2, when Cisco IPS Event Viewer (IEV) is used, exposes TCP ports used by the MySQL daemon and IEV server, which allows remote attackers to obtain "root access" to IEV via unspecified use of TCP sessions to these ports.	2009-01-22	6.8	CVE-2008-3820 CISCO
	The Certificate Authority Proxy Function (CAPF) service in Cisco			

cisco -- unified_communications_manager	Unified Communications Manager 5.x before 5.1(3e) and 6.x before 6.1(3) allows remote attackers to cause a denial of service (voice service outage) by sending malformed input over a TCP session in which the "client terminates prematurely."	2009-01-22	4.3	CVE-2009-0057 XF BID CISCO
cmsisweb -- cms_isweb	Multiple cross-site scripting (XSS) vulnerabilities in index.php in CMS ISWEB 3.0 allow remote attackers to inject arbitrary web script or HTML via (1) the stricerca parameter (aka the input field for the cerca action) or (2) the id Oggetto parameter. NOTE: some of these details are obtained from third party information.	2009-01-21	4.3	CVE-2008-5933 BID MILWORM SECUNIA
codeavalanche -- freeforum	CodeAvalanche FreeForum stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing the password via a direct request for _private/CAForum.mdb. NOTE: some of these details are obtained from third party information.	2009-01-21	5.0	CVE-2008-5932 MILWORM SECUNIA
factosystem -- factosystem_weblog	Facto stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing the password via a direct request for database/facto.mdb. NOTE: some of these details are obtained from third party information.	2009-01-21	5.0	CVE-2008-5935 XF BUGTRAQ
git -- git	gitweb/gitweb.perl in gitweb in Git 1.6.x before 1.6.0.6, 1.5.6.x before 1.5.6.6, 1.5.5.x before 1.5.5.6, 1.5.4.x before 1.5.4.7, and other versions after 1.4.3 allows local repository owners to execute arbitrary commands by modifying the diff.external configuration variable and executing a crafted gitweb query.	2009-01-20	4.6	CVE-2008-5916 MLIST MLIST MLIST MLIST
horde -- application_framework	Cross-site scripting (XSS) vulnerability in the XSS filter (framework/Text_Filter/Filter/xss.php) in Horde Application Framework 3.2.2 and 3.3, when Internet Explorer is being used, allows remote attackers to inject arbitrary web script or HTML via unknown vectors related to style	2009-01-20	4.3	CVE-2008-5917 MLIST MLIST CONFIRM

	attributes.			
ibm -- db2_universal_database	Unspecified vulnerability in IBM DB2 9.1 before FP6a and 9.5 before FP3a allows remote attackers to cause a denial of service via a crafted CONNECT data stream.	2009-01-16	5.0	CVE-2009-0172 BID CONFIRM
ibm -- db2_universal_database	Unspecified vulnerability in the server in IBM DB2 9.1 before FP6a and 9.5 before FP3a allows remote attackers to cause a denial of service (trap) via a crafted data stream.	2009-01-16	5.0	CVE-2009-0173 CONFIRM
igno_saitz -- libmikmod	libmikmod 3.1.9 through 3.2.0, as used by MikMod, SDL-mixer, and possibly other products, relies on the channel count of the last loaded song, rather than the currently playing song, for certain playback calculations, which allows user-assisted attackers to cause a denial of service (application crash) by loading multiple songs (aka MOD files) with different numbers of channels.	2009-01-20	4.3	CVE-2007-6720 CONFIRM MLIST MISC CONFIRM
igno_saitz -- libmikmod	libmikmod 3.1.11 through 3.2.0, as used by MikMod and possibly other products, allows user-assisted attackers to cause a denial of service (application crash) by loading an XM file.	2009-01-20	4.3	CVE-2009-0179 CONFIRM MLIST MISC
katywhitton -- rankem	Cross-site scripting (XSS) vulnerability in rankup.asp in Katy Whitton RankEm allows remote attackers to inject arbitrary web script or HTML via the siteID parameter.	2009-01-22	4.3	CVE-2009-0248 XF XF BID MILWORM
katywhitton -- rankem	Katy Whitton RankEm stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing credentials via a direct request for database/topsites.mdb.	2009-01-22	5.0	CVE-2009-0249 XF MILWORM
linux -- kernel	Memory leak in the keyctl_join_session_keyring function (security/keys/keyctl.c) in Linux kernel 2.6.29-rc2 and earlier allows local users to cause a denial of service (kernel memory consumption) via unknown vectors related to a "missing kfree."	2009-01-20	4.9	CVE-2009-0031 MLIST CONFIRM
mini-pub -- mini-pub	front-end/edit.php in mini-pub 0.3 and earlier allows remote attackers to read files and obtain PHP source code via a filename in the sFileName parameter.	2009-01-21	5.0	CVE-2008-5936 XF BID

	<u>username in the snippetname parameter.</u>			<u>MILWORM</u>
modxcms -- modxcms	PHP remote file inclusion vulnerability in assets/snippets/reflect/snippet.reflect.php in MODx CMS 0.9.6.2 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary PHP code via a URL in the reflect_base parameter.	2009-01-22	6.8	CVE-2008-5938 BID MILWORM CONFIRM SECUNIA
modxcms -- modxcms	Cross-site scripting (XSS) vulnerability in index.php in MODx CMS 0.9.6.2 and earlier allows remote attackers to inject arbitrary web script or HTML via a JavaScript event in the id parameter, possibly related to snippet.ditto.php.	2009-01-22	4.3	CVE-2008-5939 BID MILWORM CONFIRM
modxcms -- modxcms	SQL injection vulnerability in index.php in MODx 0.9.6.2 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the searchid parameter. NOTE: some of these details are obtained from third party information.	2009-01-22	6.8	CVE-2008-5940 BID
modxcms -- modxcms	Cross-site request forgery (CSRF) vulnerability in MODx 0.9.6.1p2 and earlier allows remote attackers to perform unauthorized actions as other users via unknown vectors.	2009-01-22	6.0	CVE-2008-5941 CONFIRM JVNDDB JVN
modxcms -- modxcms	Multiple cross-site scripting (XSS) vulnerabilities in MODx before 0.9.6.3 allow remote attackers to inject arbitrary web script or HTML via vectors related to (1) the preserveUrls function and (2) "username input." NOTE: vector 2 may be related to CVE-2008-5939.	2009-01-22	4.3	CVE-2008-5942 CONFIRM JVNDDB JVN
mozilla -- firefox	Mozilla Firefox 3.0.5 allows remote attackers to trick a user into visiting an arbitrary URL via an onclick action that moves a crafted element to the current mouse position, related to a "Status Bar Obfuscation" and "Clickjacking" attack.	2009-01-22	6.8	CVE-2009-0253 MILWORM
ryneezy -- phosheezy	Ryneezy phoSheezy 0.2 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the file containing the administrator's password hash via a direct request for config/password.	2009-01-22	5.0	CVE-2009-0250 XF MILWORM SECUNIA OSVDB
	Static code injection vulnerability in			

ryneezy -- phosheezy	admin.php in Ryneezy phoSheezy 0.2 allows remote authenticated administrators to inject arbitrary PHP code into config/footer via the footer parameter. NOTE: this can be exploited by unauthenticated attackers by leveraging CVE-2009-0250. NOTE: some of these details are obtained from third party information.	2009-01-22	6.5	CVE-2009-0251 MILWORM SECUNIA OSVDB
squirrelmail -- squirrelmail	A certain Red Hat patch for SquirrelMail 1.4.8 sets the same SQMSESSID cookie value for all sessions, which allows remote authenticated users to access other users' folder lists and configuration data in opportunistic circumstances by using the standard webmail.php interface. NOTE: this vulnerability exists because of an incorrect fix for CVE-2008-3663.	2009-01-21	6.5	CVE-2009-0030 REDHAT CONFIRM CONFIRM BID SECTRACK SECUNIA
sun -- opensolaris sun -- solaris	Unspecified vulnerability in lpadmin in Sun Solaris 10 and OpenSolaris snv_61 through snv_106 allows local users to cause a denial of service via unspecified vectors, related to enumeration of "wrong printers," aka a "Temporary file vulnerability."	2009-01-16	4.7	CVE-2009-0167 CONFIRM
sun -- opensolaris sun -- solaris	Unspecified vulnerability in ppdmgr in Sun Solaris 10 and OpenSolaris snv_61 through snv_106 allows local users to cause a denial of service via unspecified vectors, related to a failure to "include all cache files," and improper handling of temporary files.	2009-01-16	4.9	CVE-2009-0168 SUNALERT CONFIRM
sun -- java_system_access_manager	Sun Java System Access Manager 6.3 2005Q1, 7 2005Q4, and 7.1 allows remote authenticated users with console privileges to discover passwords, and obtain unspecified other "access to resources," by visiting the Configuration Items component in the console.	2009-01-16	6.0	CVE-2009-0170 BID SUNALERT CONFIRM
the_net_guys -- aspired2blog	The Net Guys ASPired2Blog stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing usernames and passwords via a direct request for admin/blog.mdb. NOTE: some of these details are obtained from third party information.	2009-01-21	5.0	CVE-2008-5931 XF MILWORM SECUNIA
	Cross-site scripting (XSS) vulnerability			

tigris -- websvn	in the getParameterisedSelfUrl function in index.php in WebSVN 2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2009-01-20	4.3	CVE-2008-5918 CONFIRM
tigris -- websvn	Directory traversal vulnerability in rss.php in WebSVN 2.0 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to overwrite arbitrary files via directory traversal sequences in the rev parameter.	2009-01-20	6.8	CVE-2008-5919 CONFIRM
trend_micro -- internet_security_2007 trend_micro -- internet_security_2008 trend_micro -- officescan	The ApiThread function in the firewall service (aka TmPfw.exe) in Trend Micro Network Security Component (NSC) modules, as used in Trend Micro OfficeScan 8.0 SP1 Patch 1 and Internet Security 2007 and 2008 17.0.1224, allows remote attackers to cause a denial of service (service crash) via a packet with a large value in an unspecified size field.	2009-01-21	5.0	CVE-2008-3864 BID SECUNIA
trend_micro -- internet_security_2007 trend_micro -- internet_security_2008 trend_micro -- officescan	The Trend Micro Personal Firewall service (aka TmPfw.exe) in Trend Micro Network Security Component (NSC) modules, as used in Trend Micro OfficeScan 8.0 SP1 Patch 1 and Internet Security 2007 and 2008 17.0.1224, relies on client-side password protection implemented in the configuration GUI, which allows local users to bypass intended access restrictions and change firewall settings by using a modified client to send crafted packets.	2009-01-21	4.6	CVE-2008-3866 BID SECUNIA SECUNIA
typo3 -- typo3	The System extension Install tool in TYPO3 4.0.0 through 4.0.9, 4.1.0 through 4.1.7, and 4.2.0 through 4.2.3 creates the encryption key with an insufficiently random seed, which makes it easier for attackers to crack the key.	2009-01-22	5.0	CVE-2009-0255 XF BID CONFIRM SECUNIA
typo3 -- typo3	Multiple cross-site scripting (XSS) vulnerabilities in TYPO3 4.0.0 through 4.0.9, 4.1.0 through 4.1.7, and 4.2.0 through 4.2.3 allow remote attackers to inject arbitrary web script or HTML via the (1) name and (2) content of indexed files to the (a) Indexed Search Engine (indexed_search) system extension; (b) unspecified test scripts in the ADOdb system extension; and (c) unspecified	2009-01-22	4.3	CVE-2009-0257 XF XF BID CONFIRM SECUNIA

	vectors in the Workspace module.			
usagi -- mynets	Cross-site scripting (XSS) vulnerability in Usagi Project MyNETS 1.2.0.1 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2008-4629.	2009-01-21	4.3	CVE-2009-0245 CONFIRM
vmware -- vmware_player vmware -- vmware_workstation	vmwarebase.dll, as used in the vmware-authd service (aka vmware-authd.exe), in VMware Workstation 6.5.1 build 126130 and earlier, and VMware Player 2.5.1 build 126130 and earlier, allows remote attackers to cause a denial of service (daemon crash) via a long (1) USER or (2) PASS command.	2009-01-20	5.0	CVE-2009-0177 SECTRACK FRSIRT SECUNIA OSVDB MILWORM
vpasp -- vp-asp_shopping_cart	VP-ASP Shopping Cart 6.50 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database containing the password via a direct request for database/shopping650.mdb. NOTE: some of these details are obtained from third party information.	2009-01-21	5.0	CVE-2008-5929 XF MILWORM
yapbb -- yapbb	PHP remote file inclusion vulnerability in include/class_yapbbcooker.php in YapBB 1.2.Beta 2 allows remote attackers to execute arbitrary PHP code via a URL in the cfgIncludeDirectory parameter.	2009-01-22	6.8	CVE-2008-5947 BID MISC

[Back to top](#)**Low Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- safari	An unspecified function in the JavaScript implementation in Apple Safari creates and exposes a "temporary footprint" when there is a current login to a web site, which makes it easier for remote attackers to trick a user into acting upon a spoofed pop-up message, aka an "in-session phishing attack." NOTE: as of 20090116, the only disclosure is a vague pre-advisory with no actionable information. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.	2009-01-20	2.1	CVE-2008-5914 MISC BID MISC MISC MISC
	An unspecified function in the JavaScript implementation in Google Chrome creates and exposes a "temporary footprint" when there is a current login to a web site, which makes it easier			CVE-2008-5915

google -- chrome	for remote attackers to trick a user into acting upon a spoofed pop-up message, aka an "in-session phishing attack." NOTE: as of 20090116, the only disclosure is a vague pre-advisory with no actionable information. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.	2009-01-20	2.1	MISC BID MISC MISC MISC
microsoft -- internet_explorer	An unspecified function in the JavaScript implementation in Microsoft Internet Explorer creates and exposes a "temporary footprint" when there is a current login to a web site, which makes it easier for remote attackers to trick a user into acting upon a spoofed pop-up message, aka an "in-session phishing attack." NOTE: as of 20090116, the only disclosure is a vague pre-advisory with no actionable information. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.	2009-01-20	2.1	CVE-2008-5912 MISC BID MISC MISC MISC
mozilla -- firefox	An unspecified function in the JavaScript implementation in Mozilla Firefox creates and exposes a "temporary footprint" when there is a current login to a web site, which makes it easier for remote attackers to trick a user into acting upon a spoofed pop-up message, aka an "in-session phishing attack." NOTE: as of 20090116, the only disclosure is a vague pre-advisory with no actionable information. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.	2009-01-20	2.1	CVE-2008-5913 MISC BID MISC MISC MISC
navboard -- navboard	Cross-site scripting (XSS) vulnerability in modules.php in NavBoard 16 (2.6.0) allows remote attackers to inject arbitrary web script or HTML via the module parameter.	2009-01-22	2.6	CVE-2008-5944 BID SECUNIA MISC
redhat -- certificate_system	Red Hat Certificate System 7.2 uses world-readable permissions for password.conf and unspecified other configuration files, which allows local users to discover passwords by reading these files.	2009-01-20	2.1	CVE-2008-2367 REDHAT CONFIRM XF BID SECTRACK SECUNIA
redhat -- certificate_system	Red Hat Certificate System 7.2 stores passwords in cleartext in the UserDirEnrollment log, the RA wizard installer log, and unspecified other debug log files, and uses weak permissions for these files, which allows local users to discover passwords by reading the files.	2009-01-20	2.1	CVE-2008-2368 REDHAT CONFIRM XF BID SECTRACK

				SECUNIA
tigris -- websvn	listing.php in WebSVN 2.0 and possibly 1.7 beta, when using an SVN authz file, allows remote authenticated users to read changelogs or diffs for restricted projects via a modified repname parameter.	2009-01-20	3.5	CVE-2009-0240 MLIST SECUNIA CONFIRM

[Back to top](#)